State Bank of India
Central Recruitment & Promotion Department
Corporate Centre, Mumbai
Email: crpd@sbi.co.in

SBI RECOGNISED AS “BEST BANK IN INDIA” FOR THE YEAR 2024 BY “GLOBAL FINANCE”

ENGAGEMENT OF SPECIALIST CADRE OFFICERS ON CONTRACT BASIS
(ADVERTISEMENT NO: CRPD/SCO/2025-26/08)
ONLINE REGISTRATION OF APPLICATION & PAYMENT OF FEES: FROM 25.08.2025 TO 15.09.2025

State Bank of India invites Online application from eligible Indian citizens for appointment to the following Specialist Cadre Officers posts. Candidates are requested to apply Online through the link given on Bank's website https://bank.sbi/careers/current- openings

1. The process of Registration is complete only when fee is deposited with the Bank through Online mode on or before the last date for payment of fee.
2. **Before applying, candidates are requested to ensure that they fulfil the eligibility criteria for the post as on the date of eligibility.**
3. **Candidate can apply for one post only.**
4. **In case of multiple applications, only the last valid (completed) application will be retained, the application fee/ intimation charge paid for other registration will stand forfeited.**
5. Candidates are required to upload all required documents (brief resume, ID proof, age proof, caste certificate, PwBD Certificate (if applicable), educational qualification, experience etc.) failing which their application/candidature will not be considered for shortlisting/ interview.
6. Short listing will be provisional without verification of documents. Candidature will be subject to verification of all details/ documents with the original when a candidate reports for interview (if called).
7. In case a candidate is called for interview and is found not satisfying the eligibility criteria **(Age, Educational Qualification and Experience etc.)** he/ she will neither be allowed to appear for the interview nor be entitled for reimbursement of any travelling expenses.
8. Candidates are advised to check Bank's website https://bank.sbi/careers regularly for details and updates (including the list of shortlisted/ selected candidates). The Call (letter/ advice), where required, will be sent by e-mail only (no hard copy will be sent).
9. ALL REVISIONS/ CORRIGENDUM (IF ANY) WILL BE HOSTED ON THE BANK'S WEBSITE ONLY.
10. In case more than one candidate scores same marks as cut-off marks in the final merit list (common marks at cut-off point), such candidates will be ranked in the merit according to their age in descending order.
11. Hard copy of application & other documents not to be sent to this office.

A: DETAILS OF POSTS/VACANCIES/SUGGESTED PLACE OF POSTING:

Sl. No.	Name of Post	Age as on 01/08/2025 (Years)				
		UR	Total	Min	Max	Suggested place of posting++
1	**Centre Head (CH)**	1	**1**	45	50	Mumbai/Navi Mumbai
2	**Senior Vice President (SVP)- Cyber Policy & Cyber Academy**	1	**1**	38	50	Mumbai/Navi Mumbai
3	**Senior Vice President (SVP)- Cyber Advisory**	1	**1**	38	50	Mumbai/Navi Mumbai
4	**Senior Vice President (SVP)- Cyber Innovation & Research**	1	**1**	38	50	Mumbai/Navi Mumbai
5	**Dy. Vice President- Cyber Policy Hub**	1	**1**	35	45	Mumbai/Navi Mumbai
6	**Dy. Vice President- Cyber Academy**	1	**1**	35	45	Mumbai/Navi Mumbai
7	**Dy. Vice President- Cyber Innovation & Simulation Lab**	1	**1**	35	45	Mumbai/Navi Mumbai
8	**Dy. Vice President- Cyber Benchmarking Hub**	1	**1**	35	45	Mumbai/Navi Mumbai
9	**Dy. Vice President- Cyber Research**	1	**1**	35	45	Mumbai/Navi Mumbai
10	**Dy. Vice President- Cyber Defense & Intelligence**	1	**1**	35	45	Mumbai/Navi Mumbai
11	**Dy. Vice President- Cyber Citizen Centric Initiative**	1	**1**	35	45	Mumbai/Navi Mumbai
12	**Dy. Vice President- Cyber Advisory**	1	**1**	35	45	Mumbai/Navi Mumbai

Abbreviation: UR- Unreserved.

++ The Bank reserves the right to transfer the services of such OECs (Officers Engaged on Contract) to any of the offices of State Bank of India in India or to depute to any of its associates/subsidiaries or any other organization depending upon the exigencies of service. Request for posting/transfer to a specific place/office may not be entertained.

IMPORTANT POINTS

i. The number of vacancies including reserved vacancies mentioned above are **provisional and may vary** according to the actual requirement of the Bank.

ii. The educational qualification prescribed for various posts are the minimum. Candidate **must possess the qualification** and **relevant full-time experience** as on specified dates.

iii. Candidate belonging to reserved category including Person with Benchmark Disabilities (PwBD) for whom no reservation has been mentioned are free to apply for vacancies announced for General category provided they fulfil all the eligibility criteria applicable to General category.

iv. The reservation (if applicable) under various categories will be as per prevailing Government of India guidelines.

v. The relevant experience certificate from the employer must contain specifically that the candidate has experience in that related field as required. **Without the production of proper experience certificate, Bank has right to cancel the candidature at any point of time.**

vi. Bank reserves the right to cancel the recruitment process entirely or for any particular post at any stage.

vii. Only those persons with benchmark disabilities would be eligible for reservation under PwBD category. "**Benchmark disability**" means a person with not less than 40% of a specified disability where specified disability has not been defined in measurable terms and includes the persons with disability, where disability has been defined in a measurable term, as certified by the certifying authority. Backlog vacancies reserved for PwBD would be filled by a person with benchmark disability in the respective category. If no suitable person from that category is available, such backlog would be filled up by interchange among other eligible PwBD candidates subject to the posts having been identified suitable for such disabilities.

viii. **TRANSFER POLICY:** The bank reserves the right to transfer the services of such officers engaged on contract (OECs) to any of the offices of State Bank of India in India or to depute to any of its associates/subsidiaries or any other organization depending upon the exigencies of service. **Any request for posting/transfer to a specific place/office may not be entertained.**

ix. **MERIT LIST:** Merit list for selection will be prepared in descending order on the basis of scores obtained in interview only. In case more than one candidate score the cut-off marks (common marks at cut-off point), such candidates will be ranked according to their age in descending order, in the merit.

x. Mere fulfilling minimum qualification and experience will not vest any right in candidate for being called for interview. the shortlisting committee constituted by the bank will decide the shortlisting parameters and thereafter, adequate number of candidates, as decided by the bank will be shortlisted and called for interview. **the decision of the bank to call the candidates for the interview shall be final. no correspondence will be entertained in this regard.**

xi. **CIBIL:** Candidates who have defaulted in repayment under any lending arrangement with Banks / NBFCs/ Financial Institutions including credit card dues and have not regularized / repaid their outstanding thereunder till the date of issuance of letter of offer of appointment by the Bank, shall not be eligible for appointment to the post. However, candidates who have regularized / repaid such outstanding on or before the date of issuance of offer of appointment, but whose CIBIL status has not been updated till then, shall, on or before the date of joining, shall have to either get the CIBIL status updated or produce the NOCs from lender to the effect that there is no outstanding with respect to the accounts adversely reflected in the CIBIL, failing which the letter of offer shall be withdrawn / cancelled. Thus, the candidates with record of default in repayment of loans/ credit card dues and/ or against whose name adverse report of CIBIL or other external agencies are available are not eligible for appointment. **Candidate are advised to check / confirm CIBIL score / status before applying.**

xii. **Candidates serving in Govt./ Quasi Govt. offices, Public Sector undertakings including Nationalized Banks and Financial Institutions and SBI Group companies are advised to submit 'No Objection Certificate' from their employer at the time of interview, failing which their candidature may not be considered and travelling expenses, if any, otherwise admissible, will not be paid**.

B. REMUNERATION & CONTRACT PERIOD:

Sl. No.	Name of Post	Annual CTC Upper Range^ (Rs In Lakhs)	Bifurcation of Annual CTC	Contract Period $
1	**Centre Head (CH) (Sl. No. 1)**	**100.00**	Fixed Pay: 90% of CTC Variable Pay#: 10% of CTC Annual Increment Band^^: 7% to 10%	**3 Years** May be renewed for further period of 2 years at the discretion of bank at mutually agreed terms and conditions. (Total engagement period should not exceed 5 years.)
2	**Senior Vice President (SVP)- (For all three posts- Sl. No. 2 to 4)**	**80.00**		
3	**Dy. Vice President (For all eight posts- Sl. No.5 to 12)**	**60.00**		

^ Annual CTC is negotiable and will depend upon experience & current emoluments of candidates in the present employment & place of posting.
$ The contract period is of 3 Years. The contract can be terminated at any time, without prejudice, by giving 90 Days' notice from either side or on payment/surrender of 90 Days' compensation amount in lieu thereof.
^^ Annual increment if any proposed second years onwards at 7-10% (Depending on performance)
 # The variable pay structure, depending on the performance of the contractual officer will be as under:

99 to 100%	**100%**
97 to 98.99 %	**90%**
94 to 96.99%	**80%**
90 to 93.99%	**70%**
Below 90%	**NIL**

OTHER PERKS: NO

C. DETAILS OF THE REQUIREMENTS OF EDUCATIONAL QUALIFICATIONS/ POST QUALIFICATION EXPERIENCES/SPECIFIC SKILLS ETC:

Post No.	Post	OTHER MANDATORY/PREFERRED QUALIFICATION/CERTFICATION (AS ON 01.08.2025)	POST QUALIFICATION WORK EXPERIENCE (AS ON 01.08.2025)	SPECIFIC SKILLS REQUIRED:
			$ Note-: Training & Teaching experience will not be counted for eligibility.	
1	**Centre Head (CH)**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** • Overall experience of 20+ years with at least 8-10 years of experience in IT/Cyber/IT Security Innovation/Cyber Research/Cyber Industry Research/IT Project management with experience of working in or setting up a CoE (Centre of Excellence). **Preferred:** • Solid understanding of banking and financial industry regulations and compliance requirements. It refers to demonstrated knowledge of key regulations and BFSI IT/Security experience including but not limited to RBI's Cyber security framework, SEBI's cyber security guidelines, data protection laws/PCI-DSS/NIST frameworks, Regulatory compliance in BFSI context. Document submission during application would not be mandatory. However, if mentioned in resume/application will be verified at the time of interview. • Excellent leadership and team management skills with the ability to motivate and develop security professionals. • Strong analytical and problem-solving abilities, with the capability to make sound decisions under pressure. • Effective communication skills, both verbal and written, to convey complex security concepts to technical and non-technical stakeholders.	• The Centre Head needs a diverse skillset, including strong leadership, strategic thinking, communication, and technical expertise to overall own the Cyber Security Centre of Excellence operations. • He must effectively manage resources, lead teams, and ensure research projects are aligned with organizational goals. Key skills include but not limited to project planning, critical thinking, data management, leadership qualities, and ethical awareness. • Knowledge of program management principles, and processes, strong interpersonal skills, people management and mentoring skills, ability to work in small teams and manage projects independently. • Excellent verbal and written communication. • Strong moral compass and that will uphold organizational values of public service, ethics, and integrity. • Customer & Citizen Centric innovative practices implementations. Ability to interact with and manage senior-level stakeholders in government, academia, and industry. • Aligning and working with objectives of SBI and enhancing its cyber security posture. • Experience in cyber security policy and practice, knowledge and experience of end to end running an innovation centric program. • Understanding and experience of cyber security technology and ability to lead team of security researchers for objective delivery. • Understanding of advanced cyber security concepts and latest technical advancements and disruptions.
2	**Senior Vice President (SVP)- Cyber Policy & Cyber Academy**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** Overall experience of 15+ years with at least 8-10 years in Cyber policy and Cyber Defense at senior level. **Preferred:** • Experience in working or managing a cyber security-related advisory environment is an added advantage. • Experience in setting up or working at a senior level in a CoE (Centre of Excellence) • Solid understanding of banking and financial industry regulations and compliance requirements. It refers to demonstrated knowledge of key regulations and BFSI IT/Security experience including but not limited to RBI's Cyber security framework, SEBI's cyber security guidelines, data protection laws/PCI-DSS/NIST frameworks, Regulatory compliance in BFSI context. Document submission during application would not be mandatory. However, if mentioned in resume/application will be verified at the time of interview.	• The SVP, Policy & Cyber Academy needs a diverse skillset, including strong leadership, strategic thinking, communication, and technical expertise. • He must effectively manage resources, lead teams, and ensure research projects are aligned with organizational goals. • Technical and Managerial skills around delivery management of Cyber related policy. • Project planning, critical thinking, data management, leadership qualities, and ethical awareness. • Knowledge of program management principles, and processes, strong interpersonal skills, people management and mentoring skills, ability to work in small teams and manage projects independently • Excellent verbal and written communication • Strong moral compass and that will uphold organizational values of public service, ethics, and integrity • Aligning and working with objectives of SBI and enhancing its cyber security posture • Experience in cyber security policy and practice, knowledge and experience of end to end running an innovation centric program. • Understanding of advanced cyber security concepts and latest technical advancements and disruptions. • Understanding of cybersecurity threats, technologies, and industry trends. • Excellent leadership, communication, and interpersonal skills. • Ability to think strategically and drive innovation in a fast-paced environment.
3	**Senior Vice President (SVP)- Cyber Advisory**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** Overall experience of 15+ years with at least 8-10 years in Cyber Threat defense at senior level. Experience in working or managing a cyber security related advisory environment is needed. **Preferred:** • Experience in working or managing a cyber security-related advisory environment • Experience in setting up or working at a senior level in a CoE is an added advantage. • Solid understanding of banking and financial industry regulations and compliance requirements. It refers to demonstrated knowledge of key regulations and BFSI IT/Security experience including but not limited to RBI's Cyber security framework, SEBI's cyber security guidelines, data protection laws/PCI-DSS/NIST frameworks, Regulatory compliance in BFSI context. Document submission during application would not be mandatory. However, if mentioned in resume/application will be verified at the time of interview.	• The SVP, Cyber Advisory needs a diverse skillset, including strong leadership, strategic thinking, communication, and technical expertise. • Ability and experience in driving outcome driven strategic advisory roles with varied stakeholders. • Strategy Development and implementation of Customer Awareness Programs • Skills to evaluate and drive Cyber Security Program effectiveness • Experience in collaboration with academic institutions, industry partners, and government agencies is highly desirable. • He must effectively manage resources, lead teams, and ensure research projects are aligned with organizational goals. • Project planning, critical thinking, data management, leadership qualities, and ethical awareness. • Knowledge of program management principles, and processes, strong interpersonal skills, people management and mentoring skills, ability to work in small teams and manage projects independently • Excellent verbal and written communication • Strong moral compass and that will uphold organizational values of public service, ethics, and integrity • Aligning and working with objectives of SBI and enhancing its cyber security posture • Understanding and experience of cyber security technology and ability to lead team of security researchers for objective delivery. • Understanding of advanced cyber security trends, threat analytics, market understanding and critical analysis capabilities. • Proven experience in leading cybersecurity initiatives for mass-based programs, gauging their effectiveness and improvements thereon. • Deep understanding of cybersecurity threats, technologies, and industry trends. • Excellent leadership, communication, and interpersonal skills.

4	**Senior Vice President (SVP)- Cyber Innovation & Research**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** Overall experience of 15+ years with at least 8-10 years in Innovation / relevant R&D experience. **Preferred:** • Experience in setting up or working at a senior level in a CoE is an added advantage. (Centre of Excellence) • Solid understanding of banking and financial industry regulations and compliance requirements. It refers to demonstrated knowledge of key regulations and BFSI IT/Security experience including but not limited to RBI's Cyber security framework, SEBI's cyber security guidelines, data protection laws/PCI-DSS/NIST frameworks, Regulatory compliance in BFSI context. Document submission during application would not be mandatory. However, if mentioned in resume/application will be verified at the time of interview.	• The SVP , Innovation & Research needs a diverse skillset, including strong leadership, strategic thinking, communication, and technical expertise. • He must effectively manage resources, lead teams, and ensure research projects are aligned with organizational goals. • Setting up an maintaining an innovation and research labs. • Experience in driving research projects and follow outcome driven approach in performing research. • Project planning, critical thinking, data management, leadership qualities, and ethical awareness. • Knowledge of program management principles, and processes, strong interpersonal skills, people management and mentoring skills, ability to work in small teams and manage projects independently • Excellent verbal and written communication • Strong moral compass and that will uphold organizational values of public service, ethics, and integrity • Aligning and working with objectives of SBI and enhancing its cyber security posture • Experience in cyber security policy and practice, knowledge and experience of end to end running an innovation centric program. • Understanding and experience of cyber security technology and ability to lead team of security researchers for objective delivery. • Understanding of advanced cyber security concepts and latest technical advancements and disruptions. • Proven experience in leading cybersecurity research and innovation teams, with a strong track record of delivering impactful solutions. • Deep understanding of cybersecurity threats, technologies, and industry trends. • Excellent leadership, communication, and interpersonal skills. • Ability to think strategically and drive innovation in a fast-paced environment. • Experience in collaboration with academic institutions, industry partners, and government agencies is highly desirable.
5	**Dy. Vice President- Cyber Policy Hub**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** • Overall experience of 12+ years with at least 8-10 years in Cyber Policy. **Preferred:** • Experience in working or managing a cyber security-related Policy / Governance environment is an added advantage. • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE is an added advantage.	A Cybersecurity Policy Hub Head requires a diverse set of skills, encompassing both technical expertise and leadership capabilities. • Experience in cyber security policy and practice, knowledge and experience of end to end running an innovation centric programs. • Ability to derive long-term cyber security Policies aligned with business objectives. • Experience in Policy advocacy and dissemination domains. • Creating, reviewing and managing metrics for Cyber Policies. • critical thinking, data management, leadership qualities, and ethical awareness. • Knowledge of program management principles, and processes, strong interpersonal skills, people management and mentoring skills, ability to work in small teams and manage projects independently • Excellent verbal and written communication • Understanding of advanced cyber security concepts and latest technical advancements and disruptions. • Knowledge of regulatory environments (especially in cybersecurity, IT, and innovation). • Staying up to date on the latest threats, technologies, and best practices in the ever-evolving cybersecurity landscape. •
6	**Dy. Vice President- Cyber Academy**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** • Overall experience of 12+ years with at least 8-10 years in Cyber Academy & knowledge dissemination roles **Preferred:** • Experience in working or managing a cyber security-related Cyber security trainings. • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE. (Centre of Excellence)	• Strong leadership and management skills, with the ability to motivate and inspire a team. • Good technical knowledge of cybersecurity domains. • Training and dissemination of technical skills , identifying needs and owning skilling and sensitization programs. • Knowledge of Cyber Labs and Modern Learning technologies. • Excellent written and verbal communication skills, with the ability to explain complex technical concepts to diverse audiences. • Strong project management skills, with the ability to plan, organize, and execute complex training initiatives. • Ability to identify and solve complex problems related to cybersecurity training and education. Ability to adapt to changing technologies and industry trends. • Exposure to public private partnership models or Centre of Excellence • Deep understanding of BFSI Sectoral Cyber Security & risks.
7	**Dy. Vice President- Cyber Innovation & Simulation Lab**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** Overall experience of 12+ years with at least 8-10 years in Cyber Innovation & Simulation **Preferred:** • Experience in working or managing a cyber Security Innovation initiatives and Simulation of cyber solutions. • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE. (Centre of Excellence)	• Strong understanding of various cybersecurity domains in futuristic cyber security technologies, emerging trends and disruptive technologies. • Proven experience in leading or supporting innovation initiatives, including ideation, prototyping, and product development. • Strong technical background with experience in areas such as cloud computing, networking, and programming languages relevant to cybersecurity. Excellent leadership, communication, and interpersonal skills to effectively collaborate with diverse teams and stakeholders. • Ability to think strategically and align innovation efforts with the organization's business objectives. Strong analytical and problem-solving skills to identify and address complex cybersecurity challenges. • Ability to adapt to changing business needs and emerging threats, demonstrating flexibility and agility in the face of new challenges. • Experience in collaboration with academic institutions, industry partners, and government agencies is highly desirable.
8	**Dy. Vice President- Cyber Benchmarking Hub**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology.	**Mandatory:** Overall experience of 12+ years with at least 8-10 years in Cyber Benchmarking undertaking Cyber analysis/ benchmarking of cyber security related processes and technologies **Preferred:** • Experience in working or managing a cyber security-related analysis of tech and products along with rating/grading of Cyber solutions.	• Experience in developing and implementing cybersecurity benchmarking programs, including the selection of appropriate metrics and methodologies. • Demonstrating the CS CoE's commitment to continuous improvement and best practices. • Strong understanding of various cybersecurity domains, including threat intelligence, incident response, security architecture, and risk management. • Proven experience in leading or supporting innovation initiatives, including ideation, prototyping, and product development.

		The preferred certifications are: CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	• Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE. (Centre of Excellence)	• Strong technical background with experience in areas such as cloud computing, networking, and programming languages relevant to cybersecurity. Excellent leadership, communication, and interpersonal skills to effectively collaborate with diverse teams and stakeholders. • Strong analytical and problem-solving skills to identify and address complex cybersecurity challenges. • Ability to adapt to changing business needs and emerging threats, demonstrating flexibility and agility in the face of new challenges.
9	**Dy. Vice President- Cyber Research**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** Overall experience of 12+ years with at least 8-10 years in Cyber Research . **Preferred:** • Experience in working on cyber security research projects. • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE. (Centre of Excellence)	• Deep understanding of cybersecurity principles, technologies, and best practices. • Proven experience in leading research and thought leadership initiatives. • Strong analytical and problem-solving skills. • Excellent communication and presentation skills. • Experience in developing and implementing cybersecurity strategies. • Knowledge of relevant industry standards and regulations. • Experience in mentoring and guiding team members • The role helps to build and maintain a high level of cybersecurity expertise within the organization and the broader community. • By contributing to the development of cybersecurity standards and best practices, the role helps to shape the future of cybersecurity. • Strong technical background with experience in areas such as cloud computing, networking, and programming languages relevant to cybersecurity. Excellent leadership, communication, and interpersonal skills to effectively collaborate with diverse teams and stakeholders. • Strong analytical and problem-solving skills to identify and address complex cybersecurity challenges.
10	**Dy. Vice President- Cyber Defense & Intelligence**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** Overall experience of 12+ years with at least 8-10 years in Cyber Defense & Intelligence. **Preferred:** • Experience in working or managing a cyber security tool related to forensics, malware analysis, Threat Hunting, Incident Response and Threat Intelligence assimilation/ creation. • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE. (Centre of Excellence)	• Communicating effectively with senior management, business units, and other stakeholders regarding cyber security risks, incidents, and mitigation plans. • Deep understanding of cybersecurity principles and best practices. • Expertise in security technologies, including firewalls, intrusion detection/prevention systems, SIEM, and endpoint protection. • Proficiency in threat intelligence platforms and tools. • Knowledge of cyber forensics and incident response procedures • Strong technical background in cybersecurity technologies and practices. • Excellent communication, interpersonal, and leadership skills. • Analyzing the likelihood that an emerging threat will impact their organization and identify where weaknesses are. • Defining reports and recommendations to the business to enable the effectiveness of mitigation and remediation efforts. • Strong understanding of cybersecurity principles, technologies, and best practices. • Ability to lead, mentor, and develop a team of cybersecurity professionals. • Ability to develop and implement a comprehensive cybersecurity strategy. • Excellent written and verbal communication skills to effectively communicate with stakeholders at all levels. • Ability to analyze complex security issues and develop effective solutions. • Ability to assess, mitigate, and manage cyber security risks. • Experience in managing and responding to cyber security incidents. • Knowledge of relevant cybersecurity standards, regulations, and best practices.
11	**Dy. Vice President- Cyber Citizen Centric Initiative**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** Overall experience of 12+ years with at least 8-10 years in Cyber Citizen Centric. **Preferred:** • Experience in working or managing a cyber security-related citizen awareness activity like Cyber related mass and niche awareness programs through varied channels/ modes. • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE. (Centre of Excellence)	• Strong leadership and management skills. • Driving and owning citizen and end user security programs and gauging their effectiveness. • Creating metrics and tracking the development of a program for outreach and Cyber user safety. • Excellent communication and interpersonal skills. • Technical expertise in relevant areas like IT, cybersecurity, and data management. • Experience in project management and program delivery. • Knowledge of relevant policies, regulations, and best practices. • Ability to work effectively in a fast-paced environment. • Experience with stakeholder engagement and relationship management. • Mentoring a team of professionals involved in citizen-centric initiatives.
12	**Dy. Vice President- Cyber Advisory**	**Mandatory:** Basic Qualifications: BE/ BTech degree in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **OR** MCA / M.E./ MTech / MSc in any discipline from a university / Institution / Board recognized by Govt. of India / approved by Govt. Regulatory bodies. **Preferred:** An advanced degree in Cybersecurity or Information Technology. **The preferred certifications are:** CISSP, CISM, CISA, CCSP, PMP, MBA (Technology Management)	**Mandatory:** Overall experience of 12+ years with at least 8-10 years in Cyber Advisory **Preferred:** • Experience in working or managing a cyber security advisory role in line of domestic and global security standards and aligned with BFSI sector centric business models. • Experience in Cybersecurity roles in IT companies, BFSI institutions, government cybersecurity setups, consulting organizations, or relevant sectors where the candidate has worked in Information Security, Cyber Policy, Innovation, Cyber Defense, or associated domains. • Experience in setting up or working in a CoE. (Centre of Excellence)	• Cyber Advisory needs a diverse skillset, including strong leadership, strategic thinking, communication, and technical expertise. • Creating advisory based on the recent threats and research. • Regularly tracking and vetting global changes in the treat landscape. • Effectively run a Cyber advisory function catering to stakeholders and enhancing engagements. • He must effectively manage resources, lead teams, and ensure research projects are aligned with organizational goals. • Understanding and experience of cyber security technology and ability to lead team of security researchers for objective delivery. • Understanding of advanced cyber security trends, threat analytics, market understanding and critical analysis capabilities. • Ability to think strategically and drive innovation in a fast-paced environment. • Cyber Advisory Team Head acts as a key leader in protecting the organization from cyber threats, ensuring business continuity, and maintaining a strong cybersecurity posture.

D. JOB PROFILE & KRAs:

Post No.	Post	Job Profile	KRA
1	**Centre Head (CH)**	Lead the operational and implementation aspects of the Centre of Excellence in Cybersecurity, State Bank of India. The objectives of the CoE are organized into three pillars: • Policy development, collaborating for regulatory policies and standards & building state of the art cyber security capacity. Building talent with program curation and collaboration with industry and academia. • Fostering Cyber research & Innovation. • Providing advice to securing BFSI ecosystem and safeguarding customers	• Set up and streamline the processes for the operationalization of the CoE initiatives, and its day-to-day management • Ensure that the CoE achieves its goals and objectives defined by Bank. • Strategize and define immediate, mid-term and long-term action plans, as well as implement and maintain program initiatives consistent with the CoE objectives. • Monitor the global cybersecurity landscape for relevant developments and breaking news • Work to assemble a team to systematically execute all CoE activities. • Track the status of deliverables, provide updates to various levels of stakeholders and take corrective actions whenever needed. • Interact with SBI Teams and research students, the cybersecurity industry ecosystem, RBI and Government agencies working in the cybersecurity space to ensure that the CoE operates as a cyber security lighthouse for innovation and research in BFSI sector.
2	**Senior Vice President (SVP)- Cyber Policy & Cyber Academy**	SVP of Policy and Cyber Academy unit will oversee the development, implementation, and management of cybersecurity policies and training programs within our Cyber Security Center of Excellence.	• **Key Responsibilities:** This role is crucial in ensuring that Cyber COE's policy hub advocates policies that strengthens the banking industry cyber security, interacts closely with regulators. The ideal candidate will possess strong leadership capabilities, extensive knowledge of cybersecurity regulations, and a proven ability to manage compliance initiatives effectively. This role also requires contouring latest content of Cyber related trainings across a multitude of stakeholders like students, practitioners, industry experts, academia and end users(customers). Key Responsibilities: • **Leadership and Management**: • Develop and implement the strategic vision for the Policy and Academy unit in alignment with the goals of the Cyber Security Center of Excellence. • Lead, mentor, and manage a team of training coordinators and policy analysts. • Foster a culture of integrity, accountability, and continual improvement within the unit. • Establish and drive industry and regulators forums for knowledge exchange **Policy Development and Implementation –** • Drive the definition of cybersecurity policies and procedures • Collaborate with internal and external stakeholders to ensure policy alignment and effectiveness. **Industry Engagement and Thought Leadership:** • Represent the organization in industry forums, conferences, and working groups related to cybersecurity policy and compliance. • Build and maintain relationships with regulatory bodies, industry partners, and other relevant entities. **Academic Collaborations** • Engage with leading universities. • Design and develop curriculum for cybersecurity capacity building • Defining learning pedagogy based on the stakeholder requirements and roles. Drive collaborations with industry experts and academia
3	**Senior Vice President (SVP)- Cyber Advisory**	The Head of Cyber Advisory will oversee the development, implementation, and management of threat intelligence, citizen centric initiatives and strategic advisory functions within the Cyber Security Center of Excellence. The ideal candidate will possess strong leadership capabilities, extensive knowledge of cybersecurity domains, and a proven ability to manage advisory initiatives effectively.	• **Strategic Leadership:** Develop and execute a strategic vision for the Cyber advisory unit that aligns with the overall goals of the Cyber Centre of Excellence. • Set up a cyber defense & Threat intelligence practice that remains at the forefront of cybersecurity practices. • **Strategy Development for Customer Awareness Programs:** Oversee the design, implementation, and continuous improvement of the customer/citizen awareness programs • **Partnerships and Collaboration:** Establish and maintain partnerships with academic institutions, industry leaders, and government agencies to enhance strategic advisory • **Quality Assurance:** Implement processes for evaluating program effectiveness, which include Cyber defense capabilities and its applications. • **Operational Excellence:** (i)Ensure the operations are efficient, with effective resource allocation and project management practices. (ii) Manage the budget, ensuring optimal use of resources for maximum impact.
4	**Senior Vice President (SVP)- Cyber Innovation & Research**	SVP of Innovation and Research Lab will lead and manage the research and innovation efforts within our Cyber Security Center of Excellence.	➢ **Key Responsibilities:** The ideal candidate will be a visionary leader with a strong background in cybersecurity research and an ability to inspire a team of researchers and technologists, with the following key responsibilities: **Leadership and Strategy:** • Develop and implement the strategic vision for the Innovation and Research Lab aligned with the broader goals of the Cyber Security Center of Excellence. • Lead, mentor, and manage a multidisciplinary team of researchers, analysts, and technologists. • Foster a culture of innovation, collaboration, and excellence within the lab. • Drive execution of CoE initiatives **Research and Development:** • Oversee the design and execution of cutting-edge research projects focused on emerging cybersecurity threats and technologies. • Identify key areas for innovation and drive initiatives that push the boundaries of cybersecurity solutions. • Collaborate with academia, industry partners, and internal stakeholders to advance research agendas and ensure technology transfer. Innovation Lab • Enable the design of innovation and research lab to ensure state-of-the-art facilities • Establish framework for research and innovation activities including infrastructure enablement, operational models, outcome measurement etc. • Drive strategic and operational relationships for implementation and operations of the lab **Innovation and Solution Development:** • Translate research findings into practical cybersecurity solutions and strategies. • Evaluate and integrate emerging technologies and methodologies into existing frameworks. • Promote the development of prototypes /toolkits and proof-of-concept demonstrations to showcase new technologies. • **Thought Leadership**: • Serve as a thought leader in the cybersecurity domain, representing the organization at industry conferences, seminars, and workshops. • Publish research findings in reputable journals and present at key industry events. • Build and maintain relationships with key stakeholders in academia, industry, and government. **Operational Excellence:** • Ensure the lab operates efficiently, with effective resource allocation and project management practices. • Monitor and report on the progress of research initiatives and innovation projects.

			• Manage the lab's budget, ensuring optimal use of resources for maximum impact.
5	**Dy. Vice President- Cyber Policy Hub**	The Cyber security Policy Hub head is a strategic leader who ensures an organization's information assets are protected by establishing and maintaining a robust cybersecurity posture. Provides guidance to an organization's employees on how to act to protect the company's sensitive information. This role also requires contouring latest content of Cyber related trainings across a multitude of stakeholders like students, practitioners, industry experts, academia and end users (customers). This is crucial role in safeguarding sensitive data and maintaining a secure operating environment. Head of Policy Hub will also oversee a team of cyber security professionals and collaborate with various stakeholders to integrate security measures policy into operational processes.	➢ **Key Responsibilities:** • **Leadership and Management:** • Develop and implement the strategic vision for the Policy in alignment with the goals of the Cyber Security Centre of Excellence. • Lead, mentor, and manage a team of policy disseminators and policy analysts. Foster a culture of integrity, accountability, and continual improvement within the unit. • Establish and drive industry and regulators forums for knowledge exchange • **Policy Development and Implementation:** • Collaborate with internal and external stakeholders to ensure policy alignment and effectiveness. • Ensure alignment with organizational goals, regulatory compliance, and industry best practices. • **Industry Engagement and Thought Leadership:** • Represent the organization in industry forums, conferences, and working groups related to cybersecurity policy and compliance. • Build and maintain relationships with regulatory bodies, industry partners, and other relevant entities • **Strategic Leadership:** • Lead the Policy Hub team and act as the primary policy advisor to CoE leadership. • Collaborate with internal departments (Legal, Risk, Compliance, IT, HR, etc.) to ensure policies are practical, enforceable, and aligned. • Drive change management initiatives related to policy adoption and awareness.
6	**Dy. Vice President- Cyber Academy**	Cyber Academy Head within a Cyber security Centre of Excellence (CSCoE) would involve leading the development and execution of cybersecurity training programs, potentially including curriculum development, instructor training, and student assessment. This role would also likely involve strategic planning, resource management, and stakeholder engagement to ensure the academy's success in building a skilled cybersecurity workforce. Key responsibilities include overseeing the academy's curriculum development, managing training delivery, and ensuring the quality and effectiveness of all cybersecurity education initiatives.	➢ **Academic Collaborations:** • Engage with leading universities and academies. • Design and develop curriculum for cyber security capacity building. • Defining learning pedagogy based on the stakeholder requirements and roles. • Drive collaborations with industry experts and academia. ➢ **Strategic Planning & Leadership:** • the strategic vision for the Cyber Academy, aligning it with the overall goals of the Cyber Security CoE. • Lead the development of a comprehensive cyber security training roadmap. • industry trends and emerging threats to ensure the academy's curriculum remains relevant and up-to-date. • Collaborate with stakeholders to identify training needs and gaps. • Strategic thinking with the ability to drive change in a fast-evolving tech landscape. • Ability to design and execute capacity building initiatives ➢ **Curriculum Development & Management:** • Oversee the design, development, and maintenance of cybersecurity training courses, workshops, and certifications. • Ensure that the curriculum covers a wide range of cybersecurity topics, including but not limited to: • Network Security • Cloud Security • Incident Response • Digital Forensics • Cybersecurity Management • Incorporate practical exercises, simulations, and real-world case studies into the training programs. ➢ **Training Delivery & Quality Assurance:** • Manage the delivery of training programs, ensuring a high-quality learning experience. • Supervise and mentor a team of trainers and instructors. • Evaluate the effectiveness of training programs through assessments, feedback mechanisms, and performance metrics. • Maintain training records and documentation. Collaboration & Stakeholder Management: • Build and maintain relationships with external partners, such as cybersecurity vendors and training providers. • Represent the Cyber Academy at industry events and conferences.
7	**Dy. Vice President- Cyber Innovation & Simulation Lab**	To lead the Innovation & Simulation Lab within the CoE, fostering a culture of experimentation, prototyping, and applied research. The role focuses on driving strategic innovation, simulating real-world cybersecurity and technology challenges, and accelerating the development and testing of emerging solutions to future-proof the organization's digital and cyber capabilities.	➢ **Innovation Strategy:** • Define a comprehensive innovation strategy aligned with the CoE's goals and the organization's overall cybersecurity objectives. ➢ **Innovation Lab:** • Enable the design of innovation and research lab to ensure state-of-the-art facilities. • Establish framework for research and innovation activities including infrastructure enablement, operational models, outcome measurement etc. • Drive strategic and operational relationships for implementation and operations of the lab. ➢ **Operational Excellence:** • Ensure the lab operates efficiently, with effective resource allocation and project management practices. • Monitor and report on the progress of research initiatives and innovation projects. • Manage the lab's budget, ensuring optimal use of resources for maximum impact. ➢ **Innovation and Solution Development:** • Translate research findings into practical cybersecurity solutions and strategies. • Evaluate and integrate emerging technologies and methodologies into existing frameworks. • Promote the development of prototypes /toolkits and proof-of-concept demonstrations to showcase new technologies. ➢ **Emerging Technologies:** • Research and assess emerging cybersecurity technologies, such as AI, machine learning, blockchain, and quantum computing, to identify potential applications and opportunities for the CoE.

			➢ **Knowledge Sharing:** • Foster a culture of knowledge sharing and collaboration within the CoE, facilitating the dissemination of best practices, research findings, and lessons learned. ➢ **External Engagement:** • Build and maintain relationships with external stakeholders, including industry experts, research institutions, and technology vendors, to stay abreast of the latest trends and foster collaboration. ➢ **Talent Development:** • Identify and nurture talent within the CoE, providing opportunities for professional development and growth in areas related to innovation and cybersecurity. ➢ **Performance Measurement:** • Define and track key performance indicators (KPIs) to measure the effectiveness of innovation initiatives and the overall impact of the CoE. ➢ **Security Posture Enhancement:** • Continuously improve the organization's security posture through the adoption of innovative solutions and best practices.
8	**Dy. Vice President- Cyber Benchmarking Hub**	To lead the Benchmarking Hub within the Center of Excellence (CoE), responsible for driving data-driven benchmarking initiatives across functions, processes, technologies, and industry peers. The role aims to foster a culture of excellence, continuous improvement, and informed decision-making by identifying performance gaps and best practices through structured benchmarking. It is responsible for establishing and maintaining a robust cybersecurity benchmarking program. This role involves defining key performance indicators (KPIs), conducting regular security assessments, and comparing an organization's cybersecurity posture against industry best practices and peers. The hub head will also lead initiatives to improve cybersecurity maturity and resilience based on benchmarking results. Security benchmarking is the practice of using simple, quantifiable metrics to establish a baseline security performance, track changes and improvements over time, and compare performance against peers, competitors, and different business units.	➢ **Developing and Implementing a Benchmarking Program:** • This includes defining relevant metrics, selecting appropriate benchmarking methodologies, and establishing a process. ➢ **Comparing Performance Against Benchmarks:** • Analyze assessment results against industry standards, best practices, and peer organizations to identify areas of strength and weakness. ➢ **Developing and Implementing Improvement Plans:** • Based on benchmarking findings, develop and implement strategies to improve cybersecurity maturity and resilience. ➢ **Fostering a Culture of Continuous Improvement:** • Promote a culture of continuous improvement in cybersecurity practices by leveraging benchmarking data to drive positive change. ➢ **Staying Current with Industry Trends:** • Continuously monitor the evolving cybersecurity landscape, including new threats, technologies, and best practices, to ensure the benchmarking program remains relevant and effective.
9	**Dy. Vice President- Cyber Research**	A Research & Thought Leadership Head for a Cybersecurity Centre of Excellence (CSCoE) focuses on driving innovation and expertise in cybersecurity. This role involves leading research initiatives, developing thought leadership content, and fostering a culture of cybersecurity excellence within the organization and externally. They are responsible for shaping the organization's perspective on emerging cybersecurity threats and best practices, and for contributing to the broader cybersecurity discourse. This role is ideal for individuals with a passion for cybersecurity, a strong research background, and a desire to make a significant impact on the cybersecurity landscape.	➢ **Thought Leadership:** • Serve as a thought leader in the cybersecurity domain, representing the organization at industry conferences, seminars, and workshops. Publish research findings in reputable journals and present at key industry events. • Build and maintain relationships with key stakeholders in academia, industry, and government. ➢ **Leading Research Initiatives:** • Identifying and prioritizing research areas based on emerging threats, industry trends, and organizational needs. • Conducting in-depth research on cybersecurity topics, including vulnerability analysis, threat intelligence, and security technologies. • Developing research methodologies and frameworks for evaluating cybersecurity risks and solutions. ➢ **Developing Thought Leadership Content:** • Defining high-quality, insightful content such as white papers, blog posts, articles, and presentations on cybersecurity topics. • Disseminating research findings and thought leadership content through various channels, including industry publications, conferences, and online platforms. • Positioning the organization as a leading authority on cybersecurity issues. ➢ **Fostering a Culture of Cybersecurity Excellence:** • Promoting a culture of continuous learning, knowledge sharing, and collaboration within the CSCoE and the broader organization. • Mentoring and guiding team members on research methodologies, cybersecurity best practices, and thought leadership development. • Encouraging the adoption of innovative cybersecurity solutions and technologies. ➢ **Engaging with Stakeholders:** • Building relationships with key stakeholders, including industry experts, academics, government agencies, and other cybersecurity professionals. • Representing the organization at industry events, conferences, and workshops. • Contributing to the development of cybersecurity standards and best practices.

			➢ **Driving Research in Cybersecurity:** • Exploring emerging technologies and their potential impact on cybersecurity. • Identifying opportunities to leverage new technologies for enhancing cybersecurity capabilities. • Developing innovative solutions to address emerging cybersecurity challenges.
10	**Dy. Vice President- Cyber Defence & Intelligence**	A Cyber Defence & Intelligence Head oversees and manages the cyber security strategy and operations for an organization, focusing on threat detection, incident response, and intelligence gathering. This role requires strong leadership, technical expertise in cybersecurity, and the ability to translate strategic goals into actionable plans. This includes building and managing a team, developing and implementing security policies and procedures, conducting threat intelligence analysis, and responding to cyber incidents. Align cyber threat intelligence with broader security and business objectives. a leadership role focused on protecting an organization's information systems and data from cyber threats.	➢ **Strategic Planning:** • Define and enhance the global cyber defence & intelligence Program. • Develop and execute the CoE's cyber defense and intelligence strategy, aligning it with the organization's overall business objectives. ➢ **Threat Intelligence & Cyber Defence:** • Ensuring effective threat detection, incident response, and vulnerability management. • Communicating effectively with senior management, business units, and other stakeholders regarding cyber security risks, incidents, and mitigation plans. • Monitor, analyze, and disseminate threat intelligence from various sources to identify emerging threats and vulnerabilities. • Conduct forensic investigations of cyber incidents to identify the root cause and attacker methods. ➢ **Stakeholder Management:** • Collaborate with other departments, such as IT, risk management, and legal, to ensure alignment and coordination of cybersecurity efforts. ➢ **Leading and Managing Teams:** • This involves overseeing cybersecurity operations, incident response, threat intelligence, and security engineering teams. ➢ **Cyber Defense:** • Advanced Malware and forensics skills • Design and Implement and Malware and Forensics Lab ➢ **Security Architecture:** • Design, implement, and maintain robust security architectures and systems to protect the organization's digital assets. ➢ **Threat Detection and Prevention:** • Proactively monitor the environment for potential threats, using various tools and techniques, and implement preventative measures. ➢ **Incident Response:** • Define and maintain incident response plans and procedures, and lead the response to cyber security incidents.
11	**Dy. Vice President-Cyber Citizen Centric Initiative**	• To lead, design, and implement citizen-centric initiatives aligned with organizational goals, ensuring services are accessible, inclusive, efficient, and impactful. The role demands strategic thinking, strong stakeholder engagement, program management capabilities, and a deep understanding of citizen needs in digital and physical governance initiatives. • Formulate and lead the vision and roadmap for citizen-centric programs under the CoE.	➢ **Developing and Implementing Cybersecurity Strategies:** • This includes creating and executing plans to protect citizens from cyber threats, such as cybercrime, online fraud, and data breaches. ➢ **Program Management:** • Overseeing the planning, execution, and delivery of citizen-centric projects, ensuring they are completed on time and within budget. • Coordinating across different departments and teams to ensure seamless integration and implementation of initiatives. • Monitoring project progress, identifying potential risks and issues, and implementing mitigation strategies. ➢ **Promoting Cyber Awareness and Literacy:** • Educating citizens about online safety, digital citizenship, and responsible online behavior is crucial. ➢ **Ensuring Access to Secure Digital Services:** • Working to make government services accessible and secure for all citizens, regardless of their technical expertise. ➢ **Fostering Collaboration:** • Working with various stakeholders, including law enforcement, technology companies, and non-profit organizations, to create a safer online environment. ➢ **Leading a Team:** • Managing and mentoring a team of cybersecurity professionals to achieve the initiative's goals. ➢ **Technical Expertise:** • Providing technical guidance and support for the design and implementation of citizen-centric solutions. • Staying up-to-date on emerging technologies and trends in areas like IoT, smart infrastructure, cybersecurity, and e-governance. • Evaluating and recommending appropriate technologies for specific citizen-facing applications.

12	**Dy. Vice President- Cyber Advisory ~~team~~**	Cyber Advisory Head is a senior-level professional who leads and manages teams focused on providing cybersecurity advice and solutions, leads a team responsible for providing strategic guidance and support to an organization on all aspects of cybersecurity.	➢ **Strategic Leadership:** • Develop and execute a strategic vision for the Cyber advisory unit that aligns with the overall goals of the Cyber Centre of Excellence. • Set up a advisory function for cyber defense & Threat intelligence practice that remains at the forefront of cybersecurity practices. ➢ **Partnerships and Collaboration:** • Establish and maintain partnerships with academic institutions, industry leaders, and government agencies to enhance strategic advisory. ➢ **Developing and Implementing Cybersecurity Strategies:** • This includes defining and maintaining a comprehensive cybersecurity roadmap, aligning it with overall business objectives, and ensuring its effective execution. ➢ **Risk Management:** • Conducting regular risk assessments, identifying vulnerabilities, and implementing mitigation strategies to minimize exposure to cyber threats. ➢ **Compliance:** • Ensuring adherence to industry standards (like ISO) and regulatory requirements through effective governance and implementation of security controls. ➢ **Team Leadership:** • Providing guidance, mentorship, and performance management to the Cyber Advisory team, fostering a collaborative and high-performing environment. ➢ **Stakeholder Management:** • Collaborating with various stakeholders, including business units, IT departments, and external partners, to promote a unified and effective cybersecurity approach. ➢ **Staying Current:** • Keeping abreast of the latest cyber threats, vulnerabilities, and security technologies to ensure the organization's defenses remain robust and up-to-date. ➢ **Promoting Cybersecurity Awareness:** • Educating employees about security best practices and fostering a culture of security awareness throughout the organization.

Remarks: KRA's: KRAs shall be assigned on joining. Job Profile mentioned above are illustrative. Role/Jobs in addition to the above mentioned may be assigned by the Bank from time to time for the above posts.

D. LEAVE: The proposed Officers engaged on Contract (OECs) shall be entitled to leave of 30 days during the financial year which will be granted by Bank for genuine and appropriate reasons.

E. NOTICE PERIOD: The contract can be terminated at any time, without prejudice, by giving 90 Days' notice from either side or on payment/surrender of 90 Days' compensation amount in lieu thereof.

F. CALL LETTER FOR INTERVIEW: Iintimation/call letter for interview will be sent by email or will be uploaded on bank's website. No hard copy will be sent.

G. SELECTION PROCESS: The selection will be based on shortlisting, Interview & CTC negotiations.

- **Shortlisting: Mere fulfilling minimum qualification and experience will not vest any right in candidate for being called for interview**. The shortlisting committee constituted by the Bank will decide the shortlisting parameters and thereafter, adequate number of candidates, as decided by the Bank, will be shortlisted for interview. The decision of the Bank to call the candidates for the interview shall be final. **No correspondence will be entertained in this regard.** The shortlisted candidates will be called for interview.
- **Interview:** Interview will carry 100 marks. The qualifying marks in interview will be decided by the Bank. No correspondence will be entertained in this regard.
- **CTC Negotiation:** CTC Negotiation will be done one-by-one, with the candidates in order of the merit list drawn on the basis of marks obtained in the interview.
- **Merit list:** Merit list for selection will be prepared in descending order on the basis of scores obtained in interview only. In case more than one candidate scores the cut-off marks (common marks at cut-off point), such candidates will be ranked according to their age in descending order, in the merit list.

(E) HOW TO APPLY: Candidates should have **valid email ID** which should be kept active till the declaration of result. It will help him/her in getting call letter/Interview advice etc. by email.

GUIDELINES FOR FILLING ONLINE APPLICATION	GUIDELINES FOR PAYMENT OF FEES
i. Candidates will be required to register themselves online through the link available on SBI website https://bank.sbi/careers/current-openings and pay the application fee using Internet Banking/ Debit Card/ Credit Card etc. ii. Candidates should first scan their latest photograph and signature. Online application will not be registered unless candidate uploads his/ her photo and signature as specified on the online registration page (under 'How to Upload Document"). iii. Candidates should fill the application carefully. Once application is filled-in completely, candidate should submit the same. In the event of candidate not being able to fill the application in one go, he can save the information already entered. When the information/ application is saved, a provisional registration number and password is generated by the system and displayed on the screen. **Candidate should note down the registration number and password.** They can re-open the saved application using registration number and password and edit the particulars, if needed. This facility of editing the saved information will be available for three times only. Once the application is filled completely, candidate should submit the same and proceed for online payment of fee. iv. **After registering online, the candidates are advised to take a printout of the system generated online application forms.**	i. Application fees and Intimation Charges (Non-refundable) is ₹750/- (₹Seven Hundred Fifty only) for General/EWS/OBC candidates and no fees/intimation charges for SC/ ST/ PwBD candidates. ii. After ensuring correctness of the particulars in the application form, candidates are required to pay the fees through payment gateway integrated with the application. No change/ edit in the application will be allowed thereafter. iii. Fee payment will have to be made online through payment gateway available thereat. The payment can be made by using Debit Card/ Credit Card/ Internet Banking etc. by providing information as asked on the screen. Transaction charges for online payment, if any, will be borne by the candidates. iv. On successful completion of the transaction, e-receipt and application form, bearing the date of submission by the candidate, will be generated which should be printed and retained by the candidate. v. If the online payment of fee is not successfully completed in first instance, please make fresh attempts to make online payment. vi. A provision is there to reprint the e-Receipt and Application form containing fee details, at later stage. vii. **Application Fee once paid will NOT be refunded on any account NOR can it be adjusted for any other examination or selection in future.**

a. Details of Document to be uploaded:

i. Recent Photograph & Signature
ii. Brief Resume (PDF)
iii. ID Proof (PDF)
iv. Proof of Date of Birth (PDF)
v. SC/ST/EWS/OBC-NCL certificate, PwBD certificates (if applicable) (PDF) (formats available in page no 13 to 16 of this advertisement)
vi. Educational Certificates: Relevant Mark-Sheets/ Degree Certificate (PDF)
vii. Experience certificates / Offer letter (PDF)
viii. Form-16/Offer Letter/Latest Salary slip from current employer (PDF)
ix. Salary account statement for last 3 months (PDF)
x. No Objection Certificate (If applicable) (PDF)
xi. Bio-data
xii. CTC Negotiation Form (In PDF)

b. Photograph file type/ size:

i. Photograph must be a recent passport style colour picture.
ii. Size of file should be between 20 kb - 50 kb and Dimensions 200 x 230 pixels (preferred)
iii. Make sure that the picture is in colour, taken against a light-coloured, preferably white, background.
iv. Look straight at the camera with a relaxed face
v. If the picture is taken on a sunny day, have the sun behind you, or place yourself in the shade, so that you are not squinting and there are no harsh shadows
vi. If you have to use flash, ensure there's no "red-eye"
vii. If you wear glasses make sure that there are no reflections and your eyes can be clearly seen.
viii. Caps, hats and dark glasses are not acceptable. Religious headwear is allowed but it must not cover your face.
ix. Ensure that the size of the scanned image is not more than 50kb. If the size of the file is more than 50 kb, then adjust the settings of the scanner such as the DPI resolution, no. of colour etc., during the process of scanning.

c. Signature file type/ size:

i. The applicant has to sign on white paper with Black Ink pen.
ii. The signature must be signed only by the applicant and not by any other person.
iii. The signature will be used to put on the Call Letter and wherever necessary.
iv. Size of file should be between 10 kb - 20 kb and Dimensions 140 x 60 pixels (preferred).
v. Ensure that the size of the scanned image is not more than 20 kb.
vi. Signature in CAPITAL LETTERS shall NOT be accepted.

d. Document file type/ size:

i. All Documents must be in PDF (except Photograph & Signature)
ii. Page size of the document to be A4
iii. Size of the file should not be exceeding 500 kb.
iv. In case of Document being scanned, please ensure it is saved as PDF and size not more than 500 kb as PDF. If the size of the file is more than 500 kb, then adjust the setting of the scanner such as the DPI resolution, no. of colors etc., during the process of scanning. Please ensure that Documents uploaded are clear and readable.

e. Guidelines for scanning of photograph/ signature/ documents:

i. Set the scanner resolution to a minimum of 200 dpi (dots per inch)
ii. Set Color to True Color
iii. Crop the image in the scanner to the edge of the photograph/ signature, then use the upload editor to crop the image to the final size (as specified above).
iv. The photo/ signature file should be JPG or JPEG format (i.e. file name should appear as: image01.jpg or image01.jpeg).
v. Image dimensions can be checked by listing the folder/ files or moving the mouse over the file image icon.
vi. Candidates using MS Windows/ MSOffice can easily obtain photo and signature in .jpeg format not exceeding 50 kb & 20 kb respectively by using MS Paint or MSOffice Picture Manager. Scanned photograph and signature in any format can be saved in .jpg format by using 'Save As' option in the File menu. The file size can be reduced below 50 kb (photograph) & 20 kb (signature) by using crop and then resize option (Please see point (i) & (ii) above for the pixel size) in the 'Image' menu. Similar options are available in another photo editor also.
vii. While filling in the Online Application Form the candidate will be provided with a link to upload his/her photograph and signature.

f. Procedure for Uploading Document:

i. There will be separate links for uploading each document.
ii. Click on the respective link "Upload"
iii. Browse & select the location where the JPG or JEPG, PDF, DOC or DOCX file has been saved.
iv. Select the file by clicking on it and click the 'Upload' button.
v. Click Preview to confirm the document is uploaded and accessible properly before submitting the application. If the file size and format are not as prescribed, an error message will be displayed
vi. Once uploaded/ submitted, the Documents uploaded cannot be edited/ changed.
vii. **After uploading the photograph/ signature in the online application form candidates should check that the images are clear and have been uploaded correctly.** In case the photograph or signature is not prominently visible, the candidate may edit his/ her application and re-upload his/ her photograph or signature, prior to submitting the form. **If the face in the photograph or signature is unclear the candidate's application may be rejected.**

(F) GENERAL INFORMATION:

I. Before applying for the post, the applicant should ensure that he/ she fulfils the eligibility and other norms mentioned above for that post as on the specified date and that the particulars furnished by him/ her are correct in all respects.

II. Candidates belonging to reserved category including, for whom no reservation has been mentioned, are free to apply for vacancies announced for General category provided they must fulfil all the eligibility conditions applicable to General category.

III. **IN CASE IT IS DETECTED AT ANY STAGE OF RECRUITMENT THAT AN APPLICANT DOES NOT FULFIL THE ELIGIBILITY NORMS AND/ OR THAT HE/ SHE HAS FURNISHED ANY INCORRECT/ FALSE INFORMATION OR HAS SUPPRESSED ANY MATERIAL FACT(S), HIS/ HER CANDIDATURE WILL STAND CANCELLED. IF ANY OF THESE SHORTCOMINGS IS/ ARE DETECTED EVEN AFTER ENGAGEMENT, HIS/ HER CONTRACTS ARE LIABLE TO BE TERMINATED.**

IV. The applicant should ensure that the application is strictly in accordance with the prescribed format and is properly filled.

V. Engagement of selected candidate is subject to his/ her being declared medically fit as per the requirement of the Bank. Such engagement will also be subject to the service and conduct rules of the Bank for such post in the Bank, in force at the time of joining the Bank.

VI. Candidates are advised to keep their e-mail ID active for receiving communication viz. call letters/ Interview date advices etc.

VII. The Bank takes no responsibility for any delay in receipt or loss of any communication.

VIII. **Candidates serving in Govt./ Quasi Govt. offices, Public Sector undertakings including Nationalized Banks and Financial Institutions and SBI Group companies are advised to submit 'No Objection Certificate' from their employer at the time of interview, failing which their candidature may not be considered and travelling expenses, if any, otherwise admissible, will not be paid**.

IX. In case of selection, candidates will be required to produce proper discharge certificate from the employer at the time of taking up the engagement.

X. Candidates are advised in their own interest to apply online well before the closing date and not to wait till the last date to avoid the possibility of disconnection / inability/ failure to log on to the website on account of heavy load on internet or website jam. SBI does not assume any responsibility for the candidates not being able to submit their applications within the last date on account of aforesaid reasons or for any other reason beyond the control of SBI.

XI. DECISION OF BANK IN ALL MATTERS REGARDING ELIGIBILITY, CONDUCT OF INTERVIEW, OTHER TESTS AND SELECTION WOULD BE FINAL AND BINDING ON ALL CANDIDATES. NO REPRESENTATION OR CORRESPONDENCE WILL BE ENTERTAINED BY THE BANK IN THIS REGARD.

XII. The applicant shall be liable for civil/ criminal consequences in case the information submitted in his/ her application are found to be false at a later stage.

XIII. Merely satisfying the eligibility norms does not entitle a candidate to be called for interview. Bank reserves the right to call only the requisite number of candidates for the interview after preliminary screening/ short-listing with reference to candidate's qualification, suitability, experience etc.

XIV. In case of multiple applications, only the last valid (completed) application will be retained, the application fee/ intimation charge paid for other registration will stand forfeited.

XV. Any legal proceedings in respect of any matter of claim or dispute arising out of this advertisement and/ or an application in response thereto can be instituted only in Mumbai and Courts/ Tribunals/ Forums at Mumbai only shall have sole and exclusive jurisdiction to try any cause/ dispute.

XVI. Outstation candidates, who may be called for interview after short-listing will be reimbursed the cost of travelling by Air (Economy Class) fare for the shortest route in India OR the actual travel cost in India (whichever is lower) on the basis of actual journey. Local conveyance like taxi/cab/personal vehicle expenses/fares will not be payable. A candidate, if found ineligible for the post will not be permitted to appear for the interview and will not be reimbursed any fare.

XVII. **Bank reserves the Right to cancel the recruitment process entirely or for any particular post at any stage.**

XVIII. **At the time of interview, the candidate will be required to provide details regarding criminal cases pending against him/her, if any. The Bank may also conduct independent verification, inter alia, including verification of Police Records, etc. The Bank reserves the right to deny the engagement depending upon such disclosure and/or independent verification.**

For any query, please write to us through link "CONTACT US/ Post Your Query" which is available on Bank's website (https://bank.sbi/web/careers)
The Bank is not liable for printing errors, if any.

Mumbai
25.08.2025

General Manager (RP & PM)

HOW TO APPLY

Login to https://bank.sbi/careers/current-openings

Scroll down and click on the respective advertisement

Download advertisement no. CRPD/SCO/2025-26/08
(Carefully read the detailed advertisement)

Apply Online
(Before final submission, please go through your application.
Corrections will not be allowed after final submission)